AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Fayetteville Division

In the Matter of the Search of	)	
	)	Case No. 5:19cm121
IN THE MATTER OF THE SEARCH OF	)	
INFORMATION ASSOCIATED WITH	)	
beaumosteller@icloud.com THAT IS STORED	)	
AT PREMISES CONTROLLED BY APPLE, INC.	)	

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe property to be searched and give its location):* **SEE ATTACHMENT "A". This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41**

located in the Western District of Arkansas, there is now concealed *(identify the person or describe the property to be seized)*: **SEE ATTACHMENT "B"**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ■ evidence of a crime;
- ■ contraband, fruits of crime, or other items illegally possessed;
- ■ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252/2252A	Possession of Child Pornography

The application is based on these facts: **See Affidavit of TFO Kevin Sears, "Attachment C"**

■ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kevin Sears, Task Force Office HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: November 12, 2019

Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, Chief United States Magistrate Judge
Printed name and title

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS
FAYETTEVILLE DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH beaumosteller@icloud.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	Case No. _____ **Filed Under Seal**

Affidavit in Support of Application for Search Warrant

I, Kevin Sears, a TFO with Homeland Security Investigations (HSI), being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application for a search warrant for information related to Apple iCloud account: **beaumosteller@icloud.com, or any account associated with Beau Mosteller,** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc., to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer (TFO) with the Department of Homeland Security, Homeland Security Investigations ("HSI"), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with Washington County Sheriff's Office since January 2007. As part of my daily duties as an HSI TFO, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. This Affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence constituting violations of Title 18, United States Code, Sections 2252/2252A Possession of Child Pornography are currently present on the item described as Attachment A.

5. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband/ fruits of these crimes further described in Attachment B.

DEFINITIONS AND AUTHORITY

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

7. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

PROBABLE CAUSE

8. In September 2019, Your Affiant received a Cyber Tip Line Report Number 52408163 from the National Center for Missing and Exploited Children (NCMEC) in reference to media files containing what was believed to be child pornography being downloaded from Snapchat. The information on the suspect media containing child pornography was submitted to the cyber tip line by Snapchat, on July 18, 2019. The incident information was categorized as being "Apparent Child Pornography" which was viewed and identified by NCMEC on all uploaded images. A total of 3 uploaded images of suspected child pornography was linked to the report. Snapchat provided the Cyber Tip Line with the following information of the user being reported:

Incident Type: Child Pornography (possession, manufacture, and distribution)

Incident Time: July 18, 2019 at 14:07:33 UTC

Chat Service/IM Client: Snapchat

Screen/User Name: jseiman7

File name: b670ddcf-ed84-409f-8321-6ab92bc0a8d_CHAT_MEDIA_1555635501968.jpeg

b670ddcf-ed84-409f-8321-6ab92bc0a8d_CHAT_MEDIA_1555635499496.jpeg

b670ddcf-ed84-409f-8321-6ab92bc0a8d_CHAT_MEDIA_1555635312892.jpeg

IP Address: 98.19.245.206 at 07-03-2019 17:22:38 UTC

Number of Uploaded Files: 3

9. On September 11, 2019, your Affiant viewed the suspect files and notes the following is depicted:

File Name: b670ddcf-ed84-409f-8321-6ab924bc0a8d_CHAT_MEDIA_1555635501968.jpeg

This image depicts what is believed to be an approximate six (6) to nine (9) year old minor female naked from the waist down and lying on her back on a bed with her legs spread open. The minor female's entire body can be seen with her vagina and anus exposed to the camera.

File Name: b670ddcf-ed84-409f-8321-6ab92bc0a8d_CHAT_MEDIA_1555635499496.jpeg

This image depicts what is believed to be an approximate six (6) to nine (9) year old minor female completely naked. She is outside in a wooded area slightly bending over a lawn chair, with her backside toward the camera, and her head turned toward the camera. The minor female's entire body can be seen with her vagina and anus exposed to the camera.

File Name: b670ddcf-ed84-409f-8321-6ab92bc0a8d_CHAT_MEDIA_1555635312892.jpeg

This image depicts what is believed to be an approximate Four (4) to six (6) year old minor female naked from the waist down and lying on her back on a bed with her legs over her head. The minor female's entire body can be seen with her vagina and anus exposed to the camera.

10. An Internet search on the origin of the IP address 98.19.245.206 found it to be issued to the Internet service provider Windstream. Documents received on or about September 5, 2019, from Windstream Compliance Center in reference to IP address 98.19.245.206 identified the IP as being assigned to Beau and Megan Mosteller through an active account number of 0006819412 with a service location at XX Pleasant Street in West Fork, AR 72774, the SUBJECT PREMISES.

11. Your Affiant conducted Department of Homeland Security (DHS) and open source database queries on the SUBJECT PREMISES which indicated Beau MOSTELLER with a date of birth in 1993 and an Arkansas driver's license bearing the last four digits 6949. The address associated to the Arkansas driver's license is listed as XX Pleasant Street, West Fork, AR 72774. Property records indicates MOSTELLER owns a 2001 Ford F-150 registered at XX Pleasant Street, West Fork, AR 72774

12. Based on the above outlined information, your Affiant sought and obtained a federal search warrant. On October 29, 2019, Your Affiant executed the federal search warrant at XX Pleasant Street in West Fork, AR. Upon execution your Affiant was informed the suspect Beau MOSTELLER recently moved to XXX Craig Street in West Fork, AR. Your Affiant went to the address and spoke with MOSTELLER.

13. MOSTELLER told your Affiant under Miranda he was using Snapchat to view pornographic material. MOSTELLER was communicating with an unknown user when they sent him a link for Mega NZ. MOSTELLER downloaded the app Mega NZ and downloaded child pornography. MOSTELLER said he used his IPhone X to download and view the child pornography. MOSTELLER felt bad about viewing child pornography and deleted everything

from his phone when he moved into his new residence. Your Affiant seized MOSTELLER'S IPhone X and gave him a receipt for the phone.

14. On November 4, 2019, your Affiant sought and obtained a search warrant for the IPhone X seized from Mosteller. On November 5, 2019, your Affiant conducted a forensic analysis of the IPhone X. Your Affiant discovered four (4) videos depicts child pornography located on MOSTELLER's IPhone X and are described as follows:

a. The first video was titled 12yo Jessica with moms toy.mp4, the file path was Beau'siPhone/var/mobile/Library/MobileDocuments/com~apple~CloudDocs/Downloads/12yo Jessica with moms toy.mp4. The MD5 hash: c763cad4a29b3ee5530bc0862c2404ce. This video is forty three (43) seconds long and depicts what is believed to be an eleven (11) to thirteen (13) year old minor female lying on a bed with her legs spread and unclothed from the waist down. The female is filming herself penetrating her vagina with a vibrator.

b. The second video was titled 2015-08-05 04.33.57.mp4, the file path was Beau's iPhone/var/mobile/Library/MobileDocuments/com~apple~CloudDocs/Downloads/2015-08-05 04.33.57.mp4. The MD5 hash was 29910c664b917ff62ae08b62acec24e3. This video is fifteen (15) seconds long and depicts what is believed to be an eleven (11) to thirteen (13) year old minor female filming herself completely naked in the shower. This video shows the breast and vagina of the minor female.

c. The third video was titled 13yo w Great Tits Selfie Vid.mp4, the file path was Beau's iPhone/var/mobile/Library/Mobile Documents/com~apple~CloudDocs/Downloads/13yo w Great Tits Selfie Vid.mp4. The MD5 hash was 62b107045ba202cd904cfd7945a555a9. This video is forty-three (43) seconds long and depicts what is believed to be an eleven (11) to thirteen (13)

year old minor female filming herself. The minor has her shirt pulled over her breast while rubbing them. The video then shows the minor naked from the waist down spreading her vagina on camera.

d. The fourth video was titled 2018-01-16 13.34.53 2.mp4, the file path was Beau's iPhone/var/mobile/Library/MobileDocuments/com~apple~CloudDocs/Downloads/2018-01-16 13.34.53 2.mp4. The MD5 hash was cdef2129f76135c15e912e2be5a20833. This video is forty-five (45) seconds long and depicts what is believed to be a twelve (12) to fourteen (14) year old minor female. The minor completely undresses herself on camera showing her breast, vagina, and buttocks.

15. The iCloud account that was logged on in MOSTELLER's phone was beaumosteller@icloud.com. Due to the file path of all four videos your Affiant believes these files are currently being stored in iCloud account beaumosteller@icloud.com.

BACKGROUND REGARDING APPLE ID AND iCLOUD[1]

16. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "iCloud: iCloud storage and backup overview," available at https://support.apple.com/kb/PH12519; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

17. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

18. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user

accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

19. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

20. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

21. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP

address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

22. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

23. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

24. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

25. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

26. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

27. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

28. Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

30. Therefore, your Affiant respectfully requests this Court to issue a search warrant authorizing the search of Apple iCloud account, **beaumosteller@icloud.com, or any account associated with Beau Mosteller** which is controlled and maintained by Apple Inc., as described in Attachment A, to seize the evidence, fruits, and instrumentalities described in Attachment B, which individually or collectively constitute a violation of Title 18, United States Code, Sections 2252/2252A, et seq, Possession of Child Pornography.

Kevin Sears, TFO
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 12th day of November, 2019.

Honorable Erin L. Wiedemann
Chief United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

This search warrant applies to all content and information associated with: **beaumosteller@icloud.com and/or Beau Mosteller** that is stored at premises controlled by Apple, Inc., a company that accepts service of legal process at located at **1 Infinite Loop, M/S 36-SU, Cupertino, CA 95104 from January 2019 until present.**

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to any request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. Any and all image or videos associated with the account, including stored or preserved or previously deleted images still accessible by Apple, any and all Meta-data or embedded data associated with the images/videos; any and all information associated with the posting IP address and/or the geolocation and identification of any devices used to save or upload images;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

g. All records pertaining to the types of service used; and

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I, including correspondence, records, documents, photographs, videos, applications, communications, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors for the above-listed crimes, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature